IB04/52475

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03104286.4

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

DEN HAAG, DEN
THE HAGUE, 28/11/03
LA HAYE, LE

Europäisches Patentamt | European Patent Office | Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 03104286.4

Anmeldetag:
Date of filing:
Date de dépôt: 20/11/03

Anmelder:
Applicant(s):
Demandeur(s):
Koninklijke Philips Electronics N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Verfahren und Einrichtung zum Verfügbarmachen von verschlüsselten digitalen Daten

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing:
Etats contractants désignés lors du dépôt: AT/BG/BE/CH/CY/CZ/DE/DK/EE/ES/FI/FR/GB/GR/HU/IE/IT/LI/LU/MC/

Bemerkungen:
Remarks:
Remarques:

Verfahren und Einrichtung zum Verfügbarmachen von verschlüsselten digitalen Daten

Die Erfindung bezieht sich auf ein Verfahren zum Verhindern einer unerwünschten Benutzung von digitalen Daten, welche digitalen Daten in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten von einer Datenquelle-Einrichtung für eine Datensenke-Einrichtung zugänglich gemacht werden und welchen digitalen Daten eine Blockierinformation zugeordnet wird, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist.

Die Erfindung bezieht sich weiters auf eine Einrichtung zum Verhindern einer unerwünschten Benutzung von digitalen Daten , welche digitalen Daten in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten von einer Datenquelle-Einrichtung für eine Datensenke-Einrichtung zugänglich machbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist.

Die Erfindung bezieht sich weiters auf eine Datensenke-Einrichtung zum Benutzen digitaler Daten, welche digitalen Daten in verschlüsselter Form verfügbar sind und welche digitalen Daten von einer Datenquelle-Einrichtung für die Datensenke-Einrichtung zugänglich machbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist.

Die Erfindung bezieht sich weiters auf eine Datenquelle-Einrichtung zum Verfügbarmachen von digitalen Daten für eine Datensenke-Einrichtung, welche digitalen Daten in verschlüsselter Form verfügbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist.

Die Erfindung bezieht sich weiters auf eine Kombinationseinrichtung mit einer Datenquelle-Einrichtung gemäß der eingangs im vierten Absatz angeführten Gattung und

mit einer Datensenke-Einrichtung gemäß der eingangs im dritten Absatz angeführten Gattung.

Eine solches Verfahren der eingangs im ersten Absatz angeführten Gattung und ein solche Einrichtung der eingangs im zweiten Absatz angeführten Gattung und eine solche Datenquelle-Einrichtung der eingangs im dritten Absatz angeführten Gattung und eine solche Datensenke-Einrichtung der eingangs im vierten Absatz angeführten Gattung und eine solche Kombinationseinrichtung der eingangs im fünften Absatz angeführten Gattung sind aus dem Patentdokument US 2003/0004885 A1 bekannt.

Bei der bekannten Einrichtung, die zum Durchführen des bekannten Verfahrens eingerichtet ist, handelt es sich um ein sogenanntes „Digital Right Management System", mit dessen Hilfe digitale Daten von einer Datenquelle-Einrichtung, die beispielsweise einem Verleiher zugeordnet ist, an eine Datensenke-Einrichtung, die beispielsweise einem Entleiher zugeordnet ist, abgebbar sind, und zwar derart, dass keine Verletzung von Urherberrechten auf die digitalen Daten eintreten soll. Zu diesem Zweck wurden die digitalen Daten von einem Besitzer der Urheberrechte um eine Benutzungsberechtigungsinformation erweitert, wodurch ein neues digitales Dokument entstand. Die Benutzungsberechtigungsinformation umfasst einerseits eine Verleiherinformation und andererseits eine Entleiherinformation, wobei die Verleiherinformation den Verleiher der digitalen Daten, von dem die digitalen Daten an einen Entleiher verliehen werden, und wobei die Entleiherinformation den Entleiher der digitalen Daten, der die digitalen Daten von dem Verleiher entleiht, repräsentiert bzw. angibt. Weiters ist in der Benutzungsberechtigungsinformation eine Blockierinformation vorgesehen, mit deren Hilfe ein weiteres Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist. Ein derart neu geschaffenes digitales Dokument wird nach einem Prüfen der zu dem jeweiligen Eigner (Owner) der digitalen Daten korrespondierenden Blockierinformation – die beispielsweise angibt, ob der Verleiher tatsächlich berechtigt ist, die digitale Information zu verleihen - an die Datensenke-Einrichtung des Entleihers übertragen.

Bei der bekannten Einrichtung besteht das Problem, dass das neu geschaffene digitale Dokument, das an einen Entleiher entliehen wird, die

Benutzungsberechtigungsinformation umfasst, sodass personenbezogenen Zugriffsrechte und/oder Verwendungsrechte direkt in dem Dokument enthalten sind, wodurch betrügerischen Manipulationen hinsichtlich der Eigentümerschaft ermöglicht sind. Weiters besteht das Problem, dass mitunter die Privatsphäre nicht gewahrt werden kann, wenn beispielsweise ein Dritter das Übertragen von einem solchen digitalen Dokument elektronisch mithört oder belauscht. Für den Fall, dass der Dritte über das reine Mithören hinausgehende Fähigkeiten besitzt, könnte er auch in der Lage sein, ein Duplikat von dem Dokument zu erstellen und andere Personen dazu berechtigen, darauf zuzugreifen und sich selbst als rechtmäßiger Eigentümer ausgeben. Ein weiteres Problem besteht darin, dass ein Verleihen der ursprünglichen digitalen Information nicht auf einfache Weise erfolgen kann - wie dies beispielsweise der Fall ist, wenn ein Tonträger von einer Person an eine andere Person verliehen wird – weil zumindest bei dem Besitzer der Urheberrechte immer ein Verändern der ursprünglichen digitalen Daten, die beispielsweise eine Audioinformation repräsentieren, durch das Erweitern der digitalen Daten um die Benutzungsberechtigungsinformation erfolgen muss bzw. bei einem Verleiher ein Verändern der mit den ursprünglichen digitalen Daten kombinierten Benutzungsberechtigungsinformation durchgeführt werden muss. Ein weiteres Problem besteht darin, dass zum Verleihen relativ aufwändige zusätzliche Maßnahmen nötig sind, wie beispielsweise auf der Seite des Verleihers eine relativ aufwändige Hardware und/oder eine Software, welche eine Verleih- bzw. Weitergabe-Berechtigung prüft bzw. eine Anzahl von Verleihvorgängen limitiert und bei Vorliegen der Verleih-Berechtigung ein digitales Dokument auf Grundlage der ursprünglichen digitalen Daten erzeugt bzw. ein bereits bestehendes digitales Dokument verändert. Weiters ist auch auf der Seite des Entleihers eine relativ aufwändige Hardware und/oder eine Software vorzusehen, welche das Benutzen eines digitalen Dokuments bzw. der in einem digitalen Dokument enthaltenen digitalen Daten ermöglicht bzw. gegebenenfalls gemäß von in der Benutzungsberechtigungsinformation enthaltenen Vorgaben des Verleihers limitiert. In beiden Fällen hat es sich daher als besonders nachteilig erwiesen, dass sowohl auf der Verleiherseite als auch auf der Entleiherseite zunächst vollständig auf ein digitales Dokument zugegriffen werden muss, was eine relativ hohe Rechenleistung und relativ große Speicherressourcen erfordert, bevor Entscheidungen betreffend die Zugriffsrechte und/oder Verwendungs- oder Benutzungsrechtrechte getroffen werden können.

Die Erfindung hat sich zur Aufgabe gestellt, die vorstehend angeführten Probleme bei einem Verfahren der eingangs im ersten Absatz angeführten Gattung und bei einer Einrichtung der eingangs im zweiten Absatz angeführten Gattung und bei einer Datensenke-Einrichtung der eingangs im dritten Absatz angeführten Gattung und bei einer Datenquelle-Einrichtung der eingangs im vierten Absatz angeführten Gattung und bei einer Kombinationseinrichtung der eingangs im fünften Absatz angeführten Gattung zu vermeiden und ein verbessertes Verfahren und eine verbesserte Einrichtung und eine verbesserte Datensenke-Einrichtung und eine verbesserte Datenquelle-Einrichtung und eine verbesserte Kombinationseinrichtung zu schaffen.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einem Verfahren gemäß der Erfindung erfindungsgemäße Merkmale vorgesehen, so dass ein Verfahren gemäß der Erfindung auf die nachfolgend angegebene Weise charakterisierbar ist, nämlich:

Verfahren zum Verhindern einer unerwünschten Benutzung von digitalen Daten, welche digitalen Daten in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten von einer Datenquelle-Einrichtung für eine Datensenke-Einrichtung zugänglich gemacht werden und welchen digitalen Daten eine Blockierinformation zugeordnet wird, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist, welches Verfahren die nachfolgend angeführten Verfahrensschritte umfasst, nämlich Verfügbarmachen einer Benutzungsberechtigungsinformation für eine Datensenke-Einrichtung, welche Benutzungsberechtigungsinformation getrennt von den digitalen Daten verfügbar gemacht wird und für ein Berechtigen des Benutzens der digitalen Daten durch die Datensenke-Einrichtung vorgesehenen ist und zumindest aus der Blockierinformation und einer Entschlüsselungsinformation besteht, welche Entschlüsselungsinformation den digitalen Daten zugeordnet ist und mit welcher Entschlüsselungsinformation die digitalen Daten entschlüsselbar sind und welche Entschlüsselungsinformation, bevor die Benutzungsberechtigungsinformation für die Datensenke-Einrichtung verfügbar gemacht wird, für die Datenquelle-Einrichtung verfügbar ist, und Entziehen der Verfügbarkeit der Entschlüsselungsinformation für die Datenquelle-Einrichtung.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einer Einrichtung

gemäß der Erfindung erfindungsgemäße Merkmale vorgesehen, so dass eine Einrichtung gemäß der Erfindung auf die nachfolgend angegebene Weise charakterisierbar ist, nämlich:

Einrichtung zum Verhindern einer unerwünschten Benutzung von digitalen Daten , welche digitalen Daten in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten von einer Datenquelle-Einrichtung für eine Datensenke-Einrichtung zugänglich machbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist, wobei Verwaltungsmittel vorgesehen sind, welche Verwaltungsmittel zum Verfügbarmachen einer getrennt von den digitalen Daten vorliegenden Benutzungsberechtigungsinformation für eine Datensenke-Einrichtung ausgebildet sind, welche Benutzungsberechtigungsinformation für ein Berechtigen des Benutzens der digitalen Daten durch die Datensenke-Einrichtung vorgesehen ist und zumindest aus der Blockierinformation und einer Entschlüsselungsinformation besteht, welche Entschlüsselungsinformation den digitalen Daten zugeordnet ist und mit welcher Entschlüsselungsinformation die digitalen Daten entschlüsselbar sind und welche Entschlüsselungsinformation, bevor die Benutzungsberechtigungsinformation für die Datensenke-Einrichtung verfügbar ist, für die Datenquelle-Einrichtung verfügbar ist, und wobei die Verwaltungsmittel zum Entziehen der Verfügbarkeit der Entschlüsselungsinformation für die Datenquelle-Einrichtung ausgebildet sind.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einer Datensenke-Einrichtung gemäß der Erfindung erfindungsgemäße Merkmale vorgesehen, so dass eine Datensenke-Einrichtung gemäß der Erfindung auf die nachfolgend angeführte Weise charakterisierbar ist, nämlich:

Datensenke-Einrichtung zum Benutzen digitaler Daten, welche digitalen Daten in verschlüsselter Form verfügbar sind und welche digitalen Daten von einer Datenquelle-Einrichtung für die Datensenke-Einrichtung zugänglich machbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist, wobei erste Verarbeitungsmittel vorgesehen sind, die unter Berücksichtigung eines ihnen zuführbaren Ermöglichungssignals, welches Ermöglichungssignal ein Verarbeiten der digitalen Daten durch die ersten

Verarbeitungsmittel ermöglicht, und unter Ausnutzung einer Entschlüsselungsinformation, welche Entschlüsselungsinformation den digitalen Daten zugeordnet ist und mit deren Hilfe die digitalen Daten entschlüsselbar sind, für das Verarbeiten der digitalen Daten ausgebildet sind, und wobei erste Prüfmittel vorgesehen sind, die erstens zum Zusammenwirken mit einer Einrichtung nach einem der Ansprüche 7 bis 12 ausgebildet sind und die zweitens zum Prüfen ausgebildet sind, ob eine Benutzungsberechtigungsinformation für die Datensenke-Einrichtung verfügbar ist, welche Benutzungsberechtigungsinformation getrennt von den digitalen Daten existiert und für das Berechtigen des Benutzens der digitalen Daten durch die Datensenke-Einrichtung vorgesehen ist und zumindest aus der Blockierinformation und der Entschlüsselungsinformation besteht und vor dem Verfügbarmachen der Benutzungsberechtigungsinformation für die Datensenke-Einrichtung der Datenquelle-Einrichtung verfügbar ist, und die drittens bei einem Vorliegen eines positiven Prüfergebnisses zum Erzeugen des Ermöglichungssignals und zum Abgeben des Ermöglichungssignals an die Verarbeitungsmittel ausgebildet sind, und wobei Blockiermittel vorgesehen sind, die unter Berücksichtigung der Blockierinformation zum Blockieren eines Verfügbarmachens der digitalen Daten für eine weitere Datensenke-Einrichtung ausgebildet sind.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einer Datenquelle-Einrichtung gemäß der Erfindung erfindungsgemäße Merkmale vorgesehen, so dass eine Datenquelle-Einrichtung gemäß der Erfindung auf die nachfolgend angeführte Weise charakterisierbar ist, nämlich:

Datenquelle-Einrichtung zum Verfügbarmachen von digitalen Daten für eine Datensenke-Einrichtung, welche digitalen Daten in verschlüsselter Form verfügbar sind und welchen digitalen Daten eine Blockierinformation zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten von der Datensenke-Einrichtung für eine weitere Datensenke-Einrichtung blockierbar ist, wobei zweite Verarbeitungsmittel vorgesehen sind, die unter Berücksichtigung eines ihnen zuführbaren Ermöglichungssignals, welches Ermöglichungssignal ein Verarbeiten der digitalen Daten durch die zweiten Verarbeitungsmittel ermöglicht, und unter Ausnutzung einer Entschlüsselungsinformation, welche Entschlüsselungsinformation den digitalen Daten zugeordnet ist und mit deren Hilfe die digitalen Daten entschlüsselbar sind, für das Verarbeiten der digitalen Daten

ausgebildet sind, und wobei zweite Prüfmittel vorgesehen sind, die erstens zum Zusammenwirken mit einer Einrichtung nach einem der Ansprüche 7 bis 12 ausgebildet sind und die zweitens zum Prüfen ausgebildet sind, ob eine Entschlüsselungsinformation für die Datenquelle-Einrichtung verfügbar ist, und die drittens bei einem Vorliegen eines positiven Prüfungsergebnisses zum Erzeugen des Ermöglichungssignals und zum Abgeben des Ermöglichungssignals an die zweiten Verarbeitungsmittel ausgebildet sind.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einer Kombinationseinrichtung gemäß der Erfindung vorgesehen, dass die Kombinationseinrichtung eine erfindungsgemäße Datenquelle-Einrichtung und eine erfindungsgemäße Datensenke-Einrichtung enthält.

Durch das Vorsehen der Maßnahmen gemäß der Erfindung ist der Vorteil erhalten, dass digitale Daten genau so von einem Verleiher an einen Entleiher verliehen werden können, wie sie ursprünglich vorliegen. Weiters ist der Vorteil erhalten, dass digitale Daten in Analogie zu einem üblichen einfachen klassischen Verleihprozess für materielle Gegenstände immer nur von demjenigen Benutzer benutzt werden können, für den gegenwärtig die Möglichkeit des Benutzens gegeben ist, weil dieser Benutzer die digitalen Daten auf analoge Weise wie einen verliehenen Gegenstand von einem Verleiher empfangen hat. Im Fall von digitalen Daten ist diese Möglichkeit des Benutzers durch das Verfügbarmachen der Benutzungsberechtigungsinformation für die Datensenke-Einrichtung des Entleihers gegeben, wobei gleichzeitig für die Datenquelle-Einrichtung des Verleihers die Entschlüsselungsinformation nicht länger zur Verfügung steht. Weiters ist durch die klare Trennung zwischen den digitalen Daten und der Benutzungsberechtigungsinformation der Vorteil erhalten, dass lediglich eine relativ kleine Datenmenge für die Benutzungsberechtigungsinformation bearbeitet bzw. verfügbar gemacht bzw. transferiert werden muss, wohingegen die üblicherweise relativ große Datenmenge für die digitalen Daten selbst nicht angetastet oder gegebenenfalls transferiert werden muss. Dies ermöglicht auch ein zentrales Verwalten bzw. Speichern der digitalen Daten auf einem für den Verleiher und den Entleiher oder ganz allgemein für Benutzer gemeinschaftlich zur Verfügung stehenden Server, auf den beide mit ihren jeweiligen Endgeräten, wie beispielsweise die Datenquelle-Einrichtung oder die Datensenke-Einrichtung oder die Kombinationseinrichtung, zugreifen können. Dadurch ist weiters der Vorteil erhalten, dass die digitalen Daten auf einem Datenträger oder über ein Online-

Service verbreitet werden können, ohne durch ein Erzeugen von Kopien der ursprünglichen digitalen Daten gegen Urheberechte auf die digitalen Daten zu verstoßen, weil die Urheberrechte insofern nicht berührt werden, als dass nur derjenige, für den die Entschlüsselungsinformation verfügbar ist, die digitalen Daten benutzen kann. Weiters ist der Vorteil erhalten, dass die Entschlüsselungsinformation zusammen mit der Blockierinformation als eine Einheit in der Benutzungsberechtigungsinformation verfügbar gemacht wird, so dass kein unberechtigtes Weiterverbreiten der Entschlüsselungsinformation erfolgen kann.

Bei den erfindungsgemäßen Lösungen kann beispielsweise vorgesehen sein, dass das Entziehen der Verfügbarkeit der Entschlüsselungsinformation für die Datenquelle-Einrichtung durch ein Verweigern von Zugriffsrechten auf die Entschlüsselungsinformation erfolgen kann. Als besonders vorteilhaft hat es sich jedoch erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 2 bzw. dem Anspruch 8 vorgesehen sind. Dadurch ist der Vorteil erhalten, dass durch das Löschen der Entschlüsselungsinformation ein gänzliches Verschwinden der Entschlüsselungsinformation sichergestellt ist, so dass ein betrügerisches Manipulieren der Zugriffsrechte zur Gänze ausgeschlossen ist, so dass die Datenquelle-Einrichtung unter gar keinen Umständen auf die digitalen Daten zugreifen bzw. diese benutzen kann.

Bei den erfindungsgemäßen Lösungen hat es sich weiters als vorteilhaft erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 3 bzw. dem Anspruch 9 vorgesehen sind. Dadurch ist der Vorteil erhalten, dass für die Datenquelle-Einrichtung eine für die Datensenke-Einrichtung charakteristische Information zur Verfügung steht, mit deren Hilfe der Verbleib der Rechte zum Benutzen der digitalen Daten auf eindeutige Weise belegbar ist und gegebenenfalls auch die Rechte zum Benutzen der digitalen Daten von der Datenquelle-Einrichtung aus zielgerichtet von der Datensenke-Einrichtung aktiv zurückgefordert werden können.

Bei den erfindungsgemäßen Lösungen hat es sich weiters als besonders vorteilhaft erweisen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 4 bzw. dem Anspruch 10 vorgesehen sind. Dadurch ist der Vorteil erhalten, dass eine persönliche oder eine berufliche oder eine auf einer anderen Basis beruhende Beziehung zwischen Benutzern mit Hilfe der Beziehungsinformation vermittelbar ist, so dass beispielsweise bei Vorliegen von einer engeren Beziehung, etwa einer freundschaftlichen Beziehung,

zwischen einem Benutzer – beispielsweise dem Entleiher - und einem anderen Benutzer – beispielsweise dem Verleiher - die Benutzungsberechtigungsinformation für den Entleiher ohne eine vorherige Anfrage bei dem Verleiher verfügbar gemacht werden kann, wohingegen bei einer distanzierten Beziehung zwischen zwei Benutzern zunächst eine solche Anfrage von dem Verleiher positiv beantwortet werden muss, also der Verleiher sein Einverständnis zum Verfügbarmachen der Benutzungsberechtigungsinformation geben muss.

Bei den erfindungsgemäßen Lösungen hat es sich weiters als besonders vorteilhaft erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 5 bzw. dem Anspruch 11. Dadurch ist der Vorteil erhalten, dass das Recht zum Benutzen der digitalen Daten auf eindeutige Weise wieder an die Datenquelle-Einrichtung zurücktransferierbar ist.

Bei den erfindungsgemäßen Lösungen hat es sich weiters als vorteilhaft erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 6 bzw. dem Anspruch 12 vorgesehen sind. Dadurch ist der Vorteil erhalten, dass ein Rückführen der Rechte zum Benutzen der digitalen Daten von dem gegenwärtigen Benutzer – beispielsweise dem Entleiher - zu dem zeitlich vorhergehenden Benutzer – beispielsweise dem Verleiher - in Abhängigkeit von einer Beziehung zwischen den beiden Benutzern erfolgen kann, so dass beispielsweise bei Vorliegen von einer näheren Beziehung zwischen den beiden Benutzern die Benutzungsberechtigungsinformation für den Entleiher ohne eine vorherige Anfrage bei dem Entleiher entzogen werden kann, wohingegen bei einer distanzierten Beziehung zwischen den beiden Benutzern zunächst eine solche Anfrage von dem Entleiher positiv beantwortet werden muss, also der Entleiher sein Einverständnis zum Entziehen der Rechte zum Benutzen der digitalen Daten geben muss.

Bei einer erfindungsgemäßen Datensenke-Einrichtung hat es sich weiters als vorteilhaft erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 14 vorgesehen sind. Dadurch kommen die im Zusammenhang mit der erfindungsgemäßen Einrichtung angeführten Vorteile auch bei der erfindungsgemäßen Datensenke-Einrichtung zum Tragen.

Bei einer erfindungsgemäßen Datenquelle-Einrichtung hat es sich weiters als vorteilhaft erwiesen, wenn zusätzlich die Maßnahmen gemäß dem Anspruch 16 vorgesehen sind. Dadurch kommen die im Zusammenhang mit der erfindungsgemäßen Einrichtung angeführten Vorteile auch bei der erfindungsgemäßen Datensenke-Einrichtung zum

Tragen.

Es sei an dieser Stelle erwähnt, dass die im Zusammenhang mit der erfindungsgemäßen Einrichtung angeführten Vorteile auch bei der erfindungsgemäßen Kombinationseinrichtung zum Tragen kommen.

Die vorstehend angeführten Aspekte und weitere Aspekte der Erfindung gehen aus den nachfolgend beschriebenen Ausführungsbeispielen hervor und sind anhand dieses Ausführungsbeispiels erläutert.

Die Erfindung wird im Folgenden anhand von zwei in den Zeichnungen dargestellten Ausführungsbeispielen weiter beschrieben, auf die die Erfindung aber nicht beschränkt ist.

Die Figur 1 zeigt auf schematische Weise in Form eines Blockschaltbilds eine ein Kommunikationssystem zum Benutzen von digitalen Daten gemäß einem ersten Ausführungsbeispiel der Erfindung.

Die Figur 2 zeigt auf schematische Weise in Form eines Blockschaltbilds ein Kommunikationssystem zum Benutzen von digitalen Daten gemäß einem zweiten Ausführungsbeispiel der Erfindung.

Die Figur 3 zeigt im Klartext einen ersten Adressbucheintrag in einem elektronischen Adressbuch betreffend einen ersten Benutzer des erfindungsgemäßen Kommunikationssystems.

Die Figur 4 zeigt auf analoge Weise wie die Figur 3 einen zweiten Adressbucheintrag in einem elektronischen Adressbuch betreffend einen zweiten Benutzer des erfindungsgemäßen Kommunikatssystems.

In der Figur 1 ist ein Kommunikationssystem 1 dargestellt, das eine Einrichtung 2 zum Verhindern einer unerwünschten Benutzung von digitalen Daten D1 oder D2 und eine erste Verarbeitungseinrichtung, die eine Datensenke-Einrichtung 3 bildet und die zum Verarbeiten der digitalen Daten D1 bzw. D2 ausgebildet ist, und eine zweite Verarbeitungseinrichtung, die eine Datenquelle-Einrichtung 4 bildet und die zum Verarbeiten der digitalen Daten D1 und D2 ausgebildet ist, aufweist. Im vorliegenden Fall

ist die erste Verarbeitungseinrichtung und die zweite Verarbeitungseinrichtung durch einen internetfähigen Fernsehapparat realisiert. Es sei an dieser Stelle erwähnt, dass die Datensenke-Einrichtung 3 und die Datenquelle-Einrichtung 4 auch durch je eine sogenannte digitale Settop-Box realisiert sein kann, die mit einem herkömmlichen Fernsehapparat in Verbindung steht. Sowohl die Einrichtung 2 als auch die Datensenke-Einrichtung 3 und die Datenquelle-Einrichtung 4 sind zum Kommunizieren über ein Computernetzwerk 5, wie beispielsweise das Internet oder ein sogenanntes Wide Area Netzwerk (WAN) oder ein sogenannte Local Area Netzwerk (LAN) oder eine Kombination aus den vorstehend genannten Netzwerken, ausgebildet. Im vorliegenden Fall sind die digitalen Daten D1 bzw. D2 unter Zuhilfenahme der Einrichtung 2 von der Datenquelle-Einrichtung 4 für die Datensenke-Einrichtung 3 zugänglich machbar, worauf nachfolgend im Detail noch eingegangen ist. Die Datensenke-Einrichtung 3 ist durch eine in ihr gespeicherte Datensenkeinformation SO auf eindeutige Weise gekennzeichnet. Die Datenquelle-Einrichtung 4 ist durch eine in ihr gespeicherte Datenquelleinformation SI auf eindeutige Weise gekennzeichnet.

In der Figur 1 ist weiters ein erster Benutzer 6 dargestellt, der mit der ersten Datensenke-Einrichtung 3 interagiert. In der Figur 1 ist weiters ein zweiter Benutzer 7 dargestellt, der mit der Datenquelle-Einrichtung 4 interagiert und der der Eigentümer (Owner) der digitalen Daten D1 und D2 ist.

Die Einrichtung 2 weist erste Kommunikationsmittel 8 und Verwaltungsmittel 9 und erste Speichermittel 10 auf. Die ersten Kommunikationsmittel 8 sind zum Kommunizieren mit den beiden Verarbeitungseinrichtungen 3 bzw. 4 und zum Zusammenwirken mit den Verwaltungsmitteln 9 ausgebildet. Die ersten Speichermittel 10 weisen einen Datenspeicherbereich 11 auf, der zum Speichern der ersten Daten D1 und der zweiten Daten D2 ausgebildet und vorgesehen ist. Die ersten Speichermittel 10 weisen weiters einen Verwaltungsspeicherbereich 12 auf, der seinerseits in einen ersten Unter-Speicherbereich zum Speichern von Eigentümerdaten OD und in einen zweiten Unter-Speicherbereich zum Speichern von Benutzungsberechtigungsdaten UGD unterteilt ist.

Die Eigentümerdaten OD sind zum Repräsentieren von einer zu den ersten Daten D1 korrespondierenden ersten Entschlüsselungsinformation DC1, die zum Entschlüsseln der ersten Daten D1 vorgesehen ist, und einer ersten Eigentümerinformation OI1, die zum Angeben des zweiten Benutzers 7 als Eigentümer der ersten Daten D1

vorgesehen ist, vorgesehen. Die Eigentümerdaten OD sind weiters vorgesehen zum Repräsentieren von einer zu den zweiten Daten D2 korrespondierenden zweiten Entschlüsselungsinformation DC2, die zum Entschlüsseln der zweiten Daten D2 vorgesehen ist, und einer zweiten Eigentümerinformation OI2, die zum Angeben des zweiten Benutzers 7 als Eigentümer der zweiten Daten D2 vorgesehen ist.

Die Benutzungsberechtigungsdaten UGD sind vorgesehen zum Repräsentieren von einer zu den ersten Daten D1 korrespondierenden ersten Benutzungsberechtigungsinformation BBI1 und von einer zu den zweiten Daten D2 korrespondierenden zweiten Benutzungsberechtigungsinformation BBI2. Die Benutzungsberechtigungsinformation BBI1 bzw. BBI2 ist für ein berechtigtes Benutzen der digitalen Daten D1 bzw. D2 durch die Datensenke-Einrichtung 3 vorgesehen und besteht zumindest aus einer Blockierinformation BL1 bzw. BL2 und der jeweiligen Entschlüsselungsinformation DC1 bzw. DC2. Die erste Entschlüsselungsinformation DC1 ist den digitalen Daten D1 zugeordnet und ist für die Datenquelle-Einrichtung 4 verfügbar, bevor die erste Entschlüsselungsinformation DC1 für die Datensenke-Einrichtung 3 verfügbar ist, also für die erste Benutzungsberechtigungsinformation BBI1 verwendet wird. Die zweite Entschlüsselungsinformation DC2 ist den digitalen Daten D2 zugeordnet und ist für die Datenquelle-Einrichtung 4 verfügbar, bevor die zweite Entschlüsselungsinformation DC2 für die Datensenke-Einrichtung 3 verfügbar ist, also für die zweite Benutzungsberechtigungseinrichtung BBI2 verwendet wird.

Die Verwaltungsmittel 9 sind zum Verfügbarmachen der getrennt von den digitalen Daten D1 bzw. D2 jeweils vorliegenden Benutzungsberechtigungsinformation BBI1 oder BBI2 für die Datensenke-Einrichtung 3 ausgebildet.

Zu diesem Zweck wird mit Hilfe der Verwaltungsmittel 9 auf Auftrag durch die Datenquelle-Einrichtung 4 oder auf Anfrage durch die Datensenke-Einrichtung 3 und gegebenenfalls nach erteilter Genehmigung durch die Datenquelle-Einrichtung 4 die jeweilige Benutzungsberechtigungsinformation BBI1 oder BBI2 erzeugt und in dem Verwaltungsspeicherbereich 12 mit Hilfe der Benutzungsberechtungsdaten UGD gespeichert. Dabei wird die Entschlüsselinformation DC1 oder DC2 aus den Eigentümerdaten OD entnommen, also kopiert, und zum Erzeugen der jeweiligen Benutzungsberechtigungsinformation BBI1 bzw. BBI2 verwendet.

Die Verwaltungsmittel 9 sind weiters zum Entziehen der Verfügbarkeit der

Entschlüsselungsinformation DC1 oder DC2 für die Datenquelle-Einrichtung 3 ausgebildet, wobei die Verwaltungsmittel 9 konkret zum Löschen der jeweiligen Entschlüsselungsinformation DC1 oder DC2 ausgebildet sind, welche Entschlüsselungsinformation DC1 oder DC2 zuvor zum Erzeugen der jeweiligen Benutzungsberechtigungsinformation BBI1 bzw. BBI2 diente. Weiters sind die Verwaltungsmittel 9 zum Merken der Datensenkeinformation SO der Datensenke-Einrichtung 3 ausgebildet, für welche die jeweiligen Daten D1 oder D2 zugänglich gemacht werden, wobei die Datensenkeinformation SO anstelle der zuvor gelöschten Entschlüsselungsinformation DC1 oder DC2 in Kombination mit der jeweiligen Eigentümerinformation OI1 oder OI2 mit Hilfe der Eigentümerdaten OD gespeichert wird.

Es sei erwähnt, dass die zu merkende Datensenkeinformation SO auch separat von dem ersten Bereich der Speichermittel 10 gespeichert werden kann, in welchem ersten Bereich zuvor die jeweilige Entschlüsselungsinformation DC1 bzw. DC2 gelöscht wurde.

Die Verwaltungsmittel 20 sind weiters zum Ergänzen der jeweiligen Benutzungsberechtigungsinformation BBI1 oder BBI2 durch die Datensenkeinformation SO ausgebildet, für welche die jeweiligen Daten D1 oder D2 zugänglich gemacht werden. Dabei bildet die Datensenkeinformation SO die Blockierinformation BL1 oder BL2, mit deren Hilfe ein Weitergeben der digitalen Daten D1 bzw. D2 an eine andere Datensenke-Einrichtung als jene, für die die jeweiligen Daten D1 bzw. D2 zugänglich gemacht wurden, blockierbar ist.

Die Verwaltungsmittel 9 sind zusätzlich zum Berücksichtigen einer ersten Beziehungsinformation RI1 ausgebildet, die in einem elektronischen Adressbuch in der Datenquelle-Einrichtung 4 gespeichert ist und mit deren Hilfe die Beziehung des zweiten Benutzer 7 der Datenquelle-Einrichtung 4 zu dem ersten Benutzer 6 der Datensenke-Einrichtung 3 definiert ist. Zu diesem Zweck sind die Verwaltungsmittel 9 dazu ausgebildet, in Abhängigkeit von der durch die erste Beziehungsinformation RI1 definierten Beziehung das Verfügbarmachen der Benutzungsberechtigungsinformation BB1 oder BBI2 für die Datensenke-Einrichtung 3 und das Entziehen der Verfügbarkeit der Entschlüsselungsinformation DC1 oder DC2 für die Datenquelle-Einrichtung 4 entweder nur auf Veranlassung durch den zweiten Benutzer 7 der Datenquelle-Einrichtung 4 – also den Eigentümer bzw. Verleiher der digitalen Daten D1 bzw. D2 - oder auch auf Veranlassung durch den ersten Benutzer 6 der Datensenke-Einrichtung 3 – also den

Entleiher der digitalen Daten D1 bzw. D2 - zu ermöglichen. Im vorliegenden Fall definiert die in der Figur 3 veranschaulichte erste Beziehungsinformation RI1, dass der erste Benutzer 6 auf Anfrage die Daten D1 oder D2 benutzen kann, und zwar ohne dass der zweite Benutzer 7 die Anfrage tatsächlich jedes Mal bestätigt, weil der erste Benutzer 6 von dem zweiten Benutzer 7 mit Hilfe der ersten Beziehungsinformation RI1 als ein sehr guter Freund eingeschätzt wird, der die digitalen Daten D1 und D2 von sich aus entleihen kann.

Die Verwaltungsmittel 20 sind weiters dazu ausgebildet, ein Beenden der Verfügbarkeit der digitalen Daten D1 oder D2 für die Datensenke-Einrichtung 3 zu ermöglichen, wobei die Verwaltungsmittel 20 zum Verfügbarmachen der zuvor für die Datensenke-Einrichtung 3 verfügbar gemachten Entschlüsselungsinformation DC1 oder DC2 für die Datenquelle-Einrichtung 4 und zum Entziehen der Verfügbarkeit der Entschlüsselungsinformation DC1 oder DC2 für die Datensenke-Einrichtung 3 ausgebildet sind. Dabei sind die Verwaltungsmittel 20 zum Entnehmen der zuvor zum Bilden der jeweiligen Benutzungsberechtigungsinformation BBI1 oder BBI2 benutzten Entschlüsselungsinformation DC1 oder DC2 aus der jeweiligen Benutzungsberechtigungsinformation BBI1 oder BBI2 und zum Speichern der jeweiligen Entschlüsselungsinformation DC1 oder DC2 an der ursprünglich dafür vorgesehenen Position innerhalb der Eigentümerdaten OD ausgebildet, wobei die zuvor an dieser Position gespeicherte Datensenkeinformation SO überschrieben wird. Die Verwaltungsmittel 20 sind weiters zum Löschen der jeweiligen Benutzungsberechtigungsinformation BBI1 oder BBI2 ausgebildet, die zuvor als Quelle für die Entschlüsselungsinformation DC1 oder DC2 diente.

Die Verwaltungsmittel 20 sind weiters zum Berücksichtigen einer in der Figur 4 veranschaulichten zweiten Beziehungsinformation RI2 ausgebildet, die in einem elektronischen Adressbuch in der Datensenke-Einrichtung 3 gespeichert ist und mit deren Hilfe die Beziehung des ersten Benutzers 6 zu dem zweiten Benutzer 7 definierbar ist. Zu diesem Zweck sind die Verwaltungsmittel 9 dazu ausgebildet, in Abhängigkeit von der durch die zweite Beziehungsinformation RI2 definierte Beziehung das Beenden der Verfügbarkeit der digitalen Daten D1 oder D2 für die Datensenke-Einrichtung 3 entweder nur auf Veranlassung des ersten Benutzers 6 der Datensenke-Einrichtung 3 – also durch den Entleiher - oder auch auf Veranlassung durch den zweiten Benutzer 7 der Datenquelle-

Einrichtung 4 – also durch den rechtmäßigen Eigentümer - zu ermöglichen. Dadurch ist erreicht, dass auch der ursprüngliche Eigentümer der digitalen Daten D1 oder D2, nämlich der zweite Benutzer 7, die an den ersten Benutzer 6 verliehene Berechtigung zum Benutzen der digitalen Daten D1oder D2 von sich aus, und vor allem ohne den ersten Benutzer 6 fragen zu müssen, zurücknehmen kann.

Die Datensenke-Einrichtung 3 weist zum Zweck des Verarbeitens der digitalen Daten D1 bzw. D2 zweite Speichermittel 13, erste Interaktionsmittel 14, erste Prüfmittel 15, erste Verarbeitungsmittel 16, zweite Kommunikationsmittel 17 und erste Blockiermittel 18 auf.

Die zweiten Kommunikationsmittel 17 sind zum Kommunizieren mit der Einrichtung 2 ausgebildet, wobei zwischen der Einrichtung 2 und der ersten Verarbeitungseinrichtung 3 Kommunikationsinformation KI austauschbar ist. Die ersten Interaktionsmittel 14 sind dazu ausgebildet, eine taktile oder audio/visuelle Interaktion mit dem ersten Benutzer 6 zu ermöglichen und zu diesem Zweck eine die Interaktion repräsentierende Interaktionsinformation IA1 mit den ersten Verarbeitungsmitteln 16 auszutauschen, mit deren Hilfe die Verarbeitungsmittel 16 steuerbar sind bzw. dem Benutzer 6 Information zugänglich machbar ist, die beispielsweise durch die digitalen Daten D1 bzw. D2 repräsentiert ist.

Die ersten Verarbeitungsmittel 16 sind weiters zum Verarbeiten der digitalen Daten D1 oder D2 ausgebildet, und zwar unter Berücksichtigung eines ihnen zuführbaren ersten Ermöglichungssignal ES1, welches erste Ermöglichungssignal ES1 ein Verarbeiten der digitalen Daten D1 oder D2 durch die ersten Verarbeitungsmittel 16 ermöglicht, und unter Ausnutzung der Entschlüsselungsinformation DC1 bzw. DC2. Die ersten Verarbeitungsmittel 16 sind weiters zum Austauschen von ersten Speicherdaten MD1 mit den ersten Speichermitteln 8 ausgebildet, welche ersten Speicherdaten MD1 gegebenenfalls beim Verarbeiten der digitalen Daten D1 bzw. D2 auftreten.

Die ersten Prüfmittel 15 sind unter Ausnutzung der zweiten Kommunikationsmittel 17 zum Zusammenwirken mit der Einrichtung 2 ausgebildet, um zu prüfen, ob eine Benutzungsberechtigungsinformation BBI1 bzw. BBI2 für die Datensenke-Einrichtung 3 verfügbar ist. Dabei wird mit Hilfe der zweiten Kommunikationsmittel 17 geprüft, ob bei der Einrichtung 2 eine Benutzungsberechtigungsinformation BBI1 bzw. BBI2 vorliegt, bei welcher die jeweilige Blockierinformation BL1 oder BL2 durch die

Datensenkeinformation SO gegeben ist, die in den zweiten Speichermitteln 13 gespeichert ist. Die ersten Prüfmittel 15 sind weiters bei einem Vorliegen eines positiven Prüfergebnisses zum Erzeugen des ersten Ermöglichungssignals ES1 und zum Abgeben des ersten Ermöglichungssignals ES1 an die ersten Verarbeitungsmittel 16 ausgebildet.

Die ersten Blockiermittel 18 sind unter Berücksichtigung der Blockierinformation BL1 oder BL2 zum Blockieren eines Verfügbarmachens der digitalen Daten D1 bzw. der D2 für eine weitere Datensenke-Einrichtung ausgebildet, die jedoch in der Figur 1 nicht dargestellt ist. Dabei ist sichergestellt, dass weder die digitalen Daten D1 bzw. D2 selbst, die als Ganzes oder in Form eines Datenstroms verarbeitet werden, noch die jeweilige der Datensenke-Einrichtung 3 verfügbare Benutzungsberechtigungsinformation BBI1 bzw. BBI2 weitergegeben werden kann bzw. durch eine andere Datensenke-Einrichtung in Kooperation mit der Datensenke-Einrichtung 3 benutzt werden kann.

Die zweiten Speichermittel 13 weisen einen ersten Adressbuchspeicherbereich 13A auf, der zum Speichern des in der Figur 4 dargestellten zweiten Adressbucheintrags 13B vorgesehen ist. Der zweite Adressbucheintrag 13B weist neben je einem Eintrag betreffend den Namen, die Telefonnummer, die E-Mail-Adresse und die Website des zweiten Benutzers 7 zusätzlich einen Eintrag betreffend die Beziehung des ersten Benutzers 6 zu dem zweiten Benutzer 7 auf, welche Beziehung durch die zweite Beziehungsinformation RI2 repräsentiert ist.

Die Datenquelle-Einrichtung 4 ist zum Verfügbarmachen der digitalen Daten D1 oder D2 für die Datensenke-Einrichtung 3 ausgebildet, was im vorliegenden Fall durch ein Bereitstellen der digitalen Daten D1 und D2 auf der Einrichtung 2 und durch ein bei der Einrichtung 2 erfolgtes Zuordnen der Eigentümerdaten OD zu den digitalen Daten D1 bzw. der D2 erfolgte.

Die Datenquelle-Einrichtung 4 weist dritte Speichermittel 19, zweite Interaktionsmittel 20, zweite Prüfmittel 21, zweite Verarbeitungsmittel 22 und dritte Kommunikationsmittel 23 auf.

Die dritten Kommunikationsmittel 23 sind zum Kommunizieren mit der Einrichtung 2 ausgebildet, wobei Kommunikationsinformation KI mit der Einrichtung 2 austauschbar ist. Die zweiten Interaktionsmittel 20 sind im wesentlichen analog zu den ersten Interaktionsmitteln 14 ausgebildet und dienen für denselben Zweck, wobei zwischen

den zweiten Interaktionsmitteln 20 und den zweiten Verarbeitungsmitteln 22 eine zweite Interaktionsinformation IA2 austauschbar ist, mit deren Hilfe eine analoge Wirkung wie mit der ersten Interaktionsinformation IA1 erzielbar ist. Die zweiten Verarbeitungsmittel 22 sind zum Verarbeiten der digitalen Daten D1 oder D2 ausgebildet, und zwar unter Berücksichtigung eines ihnen zuführbaren zweiten Ermöglichungssignals ES2, welches zweite Ermöglichungssignal ES2 ein Verarbeiten der digitalen Daten D1 und D2 durch die zweiten Verarbeitungsmittel 22 ermöglicht, und unter Ausnutzung der Entschlüsselungsinformation DC1 oder DC2.

Die zweiten Prüfmittel 21 sind unter Zuhilfenahme der dritten Kommunikationsmittel 23 zum Zusammenwirken mit der Einrichtung 2 ausgebildet, um zu prüfen, ob bei der Einrichtung 2 eine der Entschlüsselungsinformationen DC1 oder DC2 für die Datenquelle-Einrichtung 4 in den Eigentümerdaten OD verfügbar ist. Dabei wird geprüft, ob bei der Einrichtung 2 eine Entschlüsselungsinformation DC1 bzw. DC2 vorliegt, der in den Eigentümerdaten OD die Datenquelleinformation SI, die in den dritten Speichermitteln 19 gespeichert ist, als die Eigentümerinformation OI1 bzw. OI2 zugeordnet ist. Die zweiten Prüfmittel 16 sind weiters bei einem Vorliegen eines positiven Prüfergebnisses zum Erzeugen des zweiten Ermöglichungssignals ES2 und zum Abgeben des zweiten Ermöglichungssignals ES2 an die zweiten Verarbeitungsmittel 22 ausgebildet, so dass mit Hilfe der zweiten Verarbeitungsmittel 22 die digitalen Daten D1 oder D2 verarbeitbar sind, für die die jeweilige Entschlüsselungsinformation DC1 oder DC2 für die Datenquelle-Einrichtung 4 verfügbar ist.

Die dritten Speichermittel 19 weisen einen zweiten Adressbuchspeicherbereich 19A auf, der zum Speichern des in der Figur 3 dargestellten ersten Adressbucheintrags 19B vorgesehen ist. Der erste Adressbucheintrag 19B weist neben je einem Eintrag betreffend den Namen, die Telefonnummer, die E-Mail-Adresse und die Website des ersten Benutzers 6 zusätzlich einen Eintrag betreffend die Beziehung des zweiten Benutzers 7 zu dem ersten Benutzer 6 auf, welche Beziehung durch die erste Beziehungsinformation RI1 repräsentiert ist.

Gemäß den vorstehend gemachten Ausführungen ist mit Hilfe der Einrichtung 2 ein Verfahren zum Verhindern einer unerwünschten Benutzung der digitalen Daten D1 bzw. D2 durchführbar. Gemäß dem Verfahren wird zunächst eine der Benutzungsberechtigungsinformationen BBI1 oder BBI2 für die Datensenke-Einrichtung 3

verfügbar gemacht, so dass die jeweilige verfügbar gemachte Benutzungsberechtigungsinformation BBI1 bzw. BBI2 getrennt von den digitalen Daten D1 bzw. D2 verfügbar ist. Dabei erfolgt das Verfügbarmachen der Benutzungsberechtigungsinformation BBI1 bzw. BBI2 in Abhängigkeit von der bei der Datenquelle-Einrichtung 4 gespeicherten ersten Beziehungsinformation RI1 entweder nur durch den zweiten Benutzer 7 der Datenquelle-Einrichtung 4 oder auch durch den ersten Benutzer 6 der Datensenke-Einrichtung 3. Im vorliegenden Fall ist mit Hilfe der bei der Datenquelle-Einrichtung 4 gespeicherten ersten Beziehungsinformation RI1 definiert, dass das Verfügbarmachen der jeweiligen Benutzungsberechtigungsinformation BBI1 bzw. BBI2 auch durch den ersten Benutzer 6 der Datensenke-Einrichtung 3 veranlassbar ist.

Im Konkreten wird bei der Einrichtung 2 mit Hilfe der Kommunikationsinformation KI von der Datensenke-Einrichtung 3 her eine Anfrage empfangen und unter Heranziehung der bei der Datenquelle-Einrichtung 4 gespeicherten Beziehungsinformation RI1 geprüft, ob die Benutzungsberechtigungsinformation BBI1 bzw. BBI2 ohne oder mit einer expliziten Einwilligung des zweiten Benutzers 7 für die Datensenke-Einrichtung 3 verfügbar gemacht werden kann. Im vorliegenden Fall ist keine explizite Bewilligung durch den zweiten Benutzer 7 erforderlich, so dass mit Hilfe der Verwaltungsmittel 9 eine Kopie der jeweiligen Entschlüsselungsinformation DC1 bzw. DC2 in den Benutzungsberechtigungsdaten UGD korrespondierend zu den jeweiligen Daten D1 bzw. D2 erzeugt wird. Danach wird die als Basis für die Kopie dienende Entschlüsselungsinformation DC1 bzw. DC2 gelöscht und die von der Datensenke-Einrichtung 3 empfangbare bzw. abfragbare Datensenkeinformation SO an der Stelle, an der die jeweilige Entschlüsselungsinformation DC1 bzw. DC2 gelöscht wurde, in den Eigentümerdaten OD gespeichert. Weiters wird die Datensenkeinformation SO in Kombination mit der kopierten Entschlüsselungsinformation DC1 bzw. DC2 gespeichert und bildet mit dieser zusammen die jeweilige Benutzungsberechtigungsinformation BBI1 bzw. BBI2, wobei sichergestellt wird, dass die erste Benutzungsberechtigungsinformation BBI1 zu den ersten digitalen Daten D1 korrespondiert und die zweite Benutzungsberechtigungsinformation BBI2 zu den zweiten digitalen Daten D2 korrespondiert.

Durch das Löschen der zuvor für die Datenquelle-Einrichtung 4 verfügbaren Entschlüsselungsinformation DC1 bzw. DC2 wird der Datenquelle-Einrichtung 4 die

jeweilige Entschlüsselungsinformation DC1 bzw. DC2 entzogen. Durch das Speichern der Datensenkeinformation SO an der Stelle der zuvor gelöschten Entschlüsselungsinformation DC1 bzw. DC2 wird in den Eigentümerdaten OD vermerkt, an welche Datensenke-Einrichtung 3 die Berechtigung zum Benutzen der digitalen Daten D1 bzw. D2 verliehen wurde, so dass einerseits der Verbleib der Benutzungsberechtigung und andererseits die Eigentümerschaft betreffend die Benutzungsrechte auf eindeutige Weise mit Hilfe der Eigentümerdaten OD belegbar ist.

Mit Hilfe des Verfahrens zum Verhindern einer unerwünschten Benutzung von digitalen Daten ist weiters ein Beenden des Zugänglichmachens der digitalen Daten D1 bzw. D2 für die Datensenke-Einrichtung 3 durchführbar. Dabei erfolgt zunächst das Verfügbarmachen der zuvor für die Datensenke-Einrichtung 3 verfügbar gemachten Entschlüsselungsinformation DC1 bzw. DC2 für die Datenquelle-Einrichtung 4. Dies erfolgt derart, dass die in der jeweiligen Benutzungsberechtigungsinformation BBI1 bzw. BBI2 enthaltene Entschlüsselungsinformation DC1 bzw. DC2 entnommen, also kopiert, wird und die Kopie dieser Entschlüsselungsinformation DC1 bzw. DC2 nun an der Stelle in den Eigentümerdaten OD gespeichert wird, an welcher Stelle in den Eigentümerdaten OD die Datensenkeinformation SO gespeichert ist, welche Datensenkeinformation SO die Datensenke-Einrichtung 3 angibt, an welche Datensenke-Einrichtung 3 die Berechtigung zum Benutzen der digitalen Daten D1 bzw. D2 vergeben wurde. Gleichzeitig erfolgt das Entziehen der Verfügbarkeit der Entschlüsselungsinformation DC1 bzw. DC2 für die Datensenke-Einrichtung 3, wobei die entsprechende Benutzungsberechtigungsinformation BBI1 bzw. BBI2 in den Benutzungsberechtigungsdaten UGD gelöscht wird.

Auch bei dem Beenden des Zugänglichmachens der digitalen Daten D1 bzw. D2 für eine Datensenke-Einrichtung 3 erfolgt dieses Beenden in Abhängigkeit von der in der Datensenke-Einrichtung 3 gespeicherten zweiten Beziehungsinformation RI2. Im vorliegenden Fall definiert die zweite Beziehungsinformation RI2, dass ein Zurückgeben der Berechtigung zum Benutzen der jeweiligen digitalen Daten D1 bzw. D2 an den Eigentümer, also den zweiten Benutzer 7, nur auf Veranlassung des ersten Benutzers 6 erfolgen kann. Dies bedeutet, dass eine von der Datenquelle-Einrichtung 4 her mit Hilfe der Kommunikationsinformation KI bei der Einrichtung 2 eingehende Anfrage betreffend das Zurückgeben der Benutzungsberechtigung von dem ersten Benutzer 6 an den zweiten Benutzer 7, welcher der ursprüngliche Eigentümer der digitalen Daten D1 bzw. D2 ist, an

die Datensenke-Einrichtung 3 weitergeleitet wird. Diese Anfrage des zweiten Benutzers 7 muss sodann von dem ersten Benutzer 6 mit Hilfe der von der Datensenke-Einrichtung 3 her an die Einrichtung 2 kommunizierbaren Kommunikationsinformation KI positiv beantwortet werden, bevor die Verwaltungsmittel 9 das Beenden des Zugänglichmachens der digitalen Daten D1 bzw. D2 für die Datensenke-Einrichtung 3 durchführen. Es sei an dieser Stelle erwähnt, dass die zweite Beziehungsinformation RI2 auch angeben kann, dass das Beenden des Zugänglichmachens der digitalen Daten D1 bzw. D2 direkt durch den zweiten Benutzer 7 veranlasst werden kann, und zwar ohne dass der erste Benutzer 6 dies bewilligen muss. Dies hat den Vorteil, dass der zweite Benutzer 7 als Eigentümer der digitalen Daten D1 bzw. D2 die Rechte zum Benutzen der digitalen Daten D1 bzw. D2 auf aktive Weise zu ihm zurück transferieren kann.

Hinsichtlich dem Zugänglichmachen der digitalen Daten D1 bzw. D2 sei erwähnt, dass dies, wie vorstehend anhand der Figur 1 beschrieben wurde, durch ein zentrales Speichern der Entschlüsselungsinformationen DC1 und DC2 und der Benutzungsberechtigungsinformationen BBI1 und BBI2 mit Hilfe der Einrichtung 2 erfolgen kann, was jedoch voraussetzt, dass die Einrichtung 2 und die Datenquelle-Einrichtung 4 und die Datensenke-Einrichtung 3 quasi permanent miteinander kommunizieren können. Es kann jedoch auch vorgesehen sein, dass bei einem Erteilen einer Benutzungsberechtigung für die Datensenke-Einrichtung 3 bzw. für den ersten Benutzer 6 die jeweilige Benutzungsberechtigungsinformation BBI1 oder BBI2 an die Datensenke-Einrichtung 3 abgegeben wird. In diesem Zusammenhang muss jedoch gewährleistet werden, dass bei einem Entziehen der Benutzungsberechtigung die Benutzungsberechtigungsinformation BBI1 bzw. BBI2 bei der Datensenke-Einrichtung 6 gelöscht wird, was beispielsweise durch eine Kooperation der ersten Prüfmittel 15 mit den ersten Verarbeitungsmitteln 16 realisiert sein kann.

In dem in der Figur 2 dargestellten Kommunikationssystem 1 ist eine erste Kombinationseinrichtung 24 und eine zweite Kombinationseinrichtung 25 dargestellt.

Die erste Kombinationseinrichtung 24 weist die in der Figur 1 dargestellte Datenquelle-Einrichtung 4 und die in der Figur 1 dargestellte Datensenke-Einrichtung 3 und die in der Figur 1 dargestellte Einrichtung 2 zum Verhindern einer unerwünschten Benutzung der digitalen Daten D1 und D2 auf, die in der ersten Kombinationseinrichtung 24 gespeichert sind.

Die zweite Kombinationseinrichtung 25 weist ebenfalls die in der Figur 1 dargestellte Datenquelle-Einrichtung 4 und die in der Figur 1 dargestellte Datensenke-Einrichtung 3 und die in der Figur 1 dargestellte Einrichtung 2 zum Verhindern einer unerwünschten Benutzung von digitalen Daten D1' bzw. D2' auf, die in der zweiten Kombinationseinrichtung 25 gespeichert sind.

Im vorliegenden Fall bilden die Kombination aus der Datensenke-Einrichtung 3 und der Datenquelle-Einrichtung 4 Bestandteile von netzwerkfähigen Videorecordern. Es sei an dieser Stelle erwähnt, dass die Kombinationseinrichtungen 24 und 25 auch durch Audio-Aufzeichnung- und/oder Wiedergabegeräte, wie beispielsweise sogenannte MP3-Player gebildet sein können.

Durch die Integration der Datenquelle-Einrichtung 4 und der Datensenke-Einrichtung 3 in die erste Kombinationseinrichtung 24 und in die zweite Kombinationseinrichtung 25 ist erreicht, dass jede der Kombinationseinrichtungen 24 und 25 sowohl als Datenquelle zum Verfügbarmachen der in ihr gespeicherten digitalen Daten D1, D2 bzw. D1', D2' als auch als Datensenke zum Benutzen der digitalen Daten D1, D2 bzw. D1', D2' betrieben werden kann. Demgemäß weist die erste Kommunikationseinrichtung 24 eine zum eindeutigen Identifizieren vorgesehene Datenquelleinformation SI und eine Datensenkeinformation SO auf, die jedoch in der Figur 2 nicht explizit dargestellt sind. Gleiches gilt für die zweite Kombinationseinrichtung 25.

Weiters ist durch die Integration der Einrichtung 2 in jeder der zwei Kombinationseinrichtungen 24 und 25 erreicht, dass das Verhindern einer unerwünschten Benutzung der in der jeweiligen Kombinationseinrichtung 24 und 25 gespeicherten digitalen Daten D1, D2 bzw. D1', D2' auf zuverlässige und autonome Weise realisiert ist, ohne dass ein Server zum Bereitstellen der digitalen Daten D1 , D2 bzw. D1', D2', der in der Figur 1 mit Hilfe der Einrichtung 2 realisiert ist, nötig ist.

Auch im vorliegenden Fall ist vorgesehen, dass die bei den Kombinationseinrichtungen 24 und 25 erzeugbaren Benutzungsberechtigungsinformationen BBI1, BBI2 bzw. BBI1', BBI2' in den jeweiligen Speichermitteln 10 der Einrichtung 2 der jeweiligen Kombinationseinrichtung 24 oder 25 aufbewahrt werden und von den Verwaltungsmitteln verwaltet werden. Es kann jedoch auch vorgesehen sein, dass zum Erteilen der jeweiligen Benutzungsberechtigung die Benutzungsberechtigungsinformationen BBI1 bzw. BBI2 an die Kombinationseinrichtung

25 und die Benutzungsberechtigungsinformationen BBI1' bzw. BBI2' an die Kombinationseinrichtung 24 abgebbar sind. Auch in diesem Fall muss implementiert sein, dass bei einem Entziehen der jeweiligen Benutzungsberechtigung die zuvor an die jeweilige Kombinationseinrichtung 24 oder 25 übergebenen Benutzungsberechtigungsinformationen BBI1 bzw. BBI2 und BBI1' bzw. BBI2' dort gelöscht werden, damit sie nach dem Entziehen der Benutzungsberechtigung nicht weiterhin zur Verfügung stehen. Für den Fall, dass die beiden Kombinationseinrichtungen 24 und 25 nicht immer miteinander in Kommunikationsverbindung stehen, kann das gegenseitige Prüfen bzw. Anpassen der Berechtigung oder Nichtberechtigung zum Benutzen der digitalen Daten D1, D2, D1' und D2' immer dann erfolgen, wenn eine Kommunikation zwischen den Kombinationseinrichtungen möglich ist.

Sowohl die erste Kombinationseinrichtung 24 als auch die zweite Kombinationseinrichtung 25 weist kombinierte Verarbeitungsmittel 16, 22 auf. Die Verwaltungsmittel 9 sind den kombinierten Verarbeitungsmitteln 16, 22 und den Prüfmitteln 15, 21 und den Blockiermitteln 18 hierarchisch übergeordnet und mit Hilfe von Software implementiert, so dass es zu keiner Verletzung von Benutzungsrechten bei einer der zwei Kombinationseinrichtungen 24 und 25 kommen kann.

Die Kombinationseinrichtungen 24 und 25 weisen gemäß der Ausbildung der Datensenke-Einrichtung 3 und gemäß der Ausbildung der Datenquelle-Einrichtung sowohl erste Kommunikationsmittel 17 als auch zweite Kommunikationsmittel 23 auf, die in der Figur 2 getrennt voneinander dargestellt sind. Es versteht sich für den Fachmann jedoch von selbst, dass die Kommunikationsmittel 17 und 23 auch gemeinsam in einer Einheit realisiert sein können.

Es sei erwähnt, dass bei einer erfindungsgemäßen Lösung auch vorgesehen sein kann, dass die Eigentümerdaten OD und die Benutzungsberechtigungsdaten UGD derart zusammengefasst sind, dass die Entschlüsselungsinformation DC1 bzw. DC2 nur ein einziges Mal existieren muss und keine Kopie zum Erzeugen der Benutzungsberechtigungsinformation BBI1 bzw. BBI2 erforderlich ist. Bei einer solchen Lösung wird beispielsweise das Entziehen der jeweiligen Entschlüsselungsinformation DC1 bzw. DC2 für die Datenquelle-Einrichtung 4 dadurch erreicht, dass als Blockierinformation BL1 bzw. BL2 die Datensenkeinformation SO gespeichert wird. Mit Hilfe der Verwaltungsmittel 9 kann dann sichergestellt werden, dass so bald eine gültige

Blockierinformation BL1 bzw. BL2 vorliegt, die Datenquelle-Einrichtung 4 nicht mehr auf die Entschlüsselungsinformation DC1 bzw. DC2 zugreifen kann. In Analogie dazu kann das Zurücktransferieren der Rechte zum Benutzen der digitalen Daten D1 bzw. D2 dadurch erreicht werden, dass die als Blockierinformation BL1 bzw. BL2 gespeicherte Datensenkeinformation SO durch die Eigentümerinformation OI1 bzw. OI2 überschrieben wird. Auch in diesem Fall ist eindeutig feststellbar, wer der tatsächliche Eigentümer der digitalen Daten D1 bzw. D2 ist, weil die Eigentümerinformation OI1 bzw. OI2 niemals verändert wird und die Blockierinformation für die Datensenke-Einrichtung 3 nach wie vor ihre Bedeutung behält. In diesem Zusammenhang sei erwähnt, dass das Zurücktransferieren der Rechte zum Benutzen der digitalen Daten D1 bzw. D2 auch dadurch erfolgen kann, dass die als Blockierinformation BL1 bzw. BL2 gespeicherte Datensenkeinformation SO einfach gelöscht wird, so dass nur mehr die Entschlüsselungsinformation DC1 und die Eigentümerinformation OI1 erhalten bleiben, wenn die Datenquelle-Einrichtung 4 zum Benutzen der digitalen Daten D1 bzw. D2 berechtigt sein soll. Gleiches gilt auch für das Ausführungsbeispiel gemäß Figur 2.

Es sei an dieser Stelle erwähnt, dass auch eine Datenquelle-Einrichtung 4 ohne eine Datensenke-Einrichtung 3, jedoch mit der Einrichtung 2 vorgesehen sein kann. In Analogie dazu sei erwähnt, dass auch eine Datensenke-Einrichtung 3 ohne eine Datenquelle-Einrichtung 4, jedoch mit der Einrichtung 2 vorgesehen sein kann.

Es sei erwähnt, dass die Verfügbarkeit der Benutzungsberechtigungsinformation bzw. der Entschlüsselungsinformation auch nur zeitlich begrenzt vergeben werden kann, wobei ein Interessent, der beispielsweise die einen Film repräsentierenden Daten entleihen und betrachten will, die Berechtigung dazu anfordert und wobei diese Berechtigung nachfolgend erteilt wird, jedoch diese Berechtigung nur so lange verfügbar bleibt, wie der Interessent tatsächlich den Film ansieht, so dass nach Beendigung des Films die Berechtigung automatisch wieder entzogen bzw. zurückgegeben bzw. gelöscht wird. Demgemäß steht dem Interessenten bzw. Entleiher und Betrachter des Films die Berechtigung nur temporär zur Verfügung.

Es sei erwähnt, dass die Datensenkeinforation SO und/oder die Datenquelleinformation SI auch temporär bei der jeweiligen Verarbeitungseinrichtung 3 bzw. 4 vorliegen kann, wie dies beispielweise der Fall ist, wenn sich einer der zwei Benutzer 6 oder 7 mit Hilfe einer sogenannten Chipkarte, in der eine den Benutzer auf

eindeutige Weise identifizierende Benutzerinformation gespeichert ist, gegenüber der jeweiligen Verarbeitungseinrichtung 3 oder 4 identifiziert und die Verarbeitungseinrichtung 3 bzw. 4 die mit Hilfe der Chipcard verfügbare Benutzerinformation entweder als Datensenkeinformation SO oder als Datenquelleinformation SI verwendet, solange ihr die Chipkarte beispielweise mit Hilfe einer sogenannten Leseinrichtung zugänglich ist.

Es sei erwähnt, dass, obwohl in der Figur 1 nur eine einzige Datenquelle-Einrichtung 4 und eine einzige Datensenke-Einrichtung 3 dargestellt sind, auch mehrere Datenquelle-Einrichtungen 4, 4', 4'' usw. und/oder mehrere Datensenke-Einrichtungen 3, 3', 3'' usw. vorhanden sein können, wobei mit Hilfe der Einrichtung 2 und insbesondere mit Hilfe der Verwaltungsmittel 9 das Berechtigen zum Benutzen der von den jeweiligen Datenquelle-Einrichtungen 4, 4', 4'' usw. für die Datensenke-Einrichtung 3, 3', 3'' usw. bereitgestellten digitalen Daten verwaltet wird.

Weiters sei erwähnt, dass die digitalen Daten D1 bzw. D2 verschiedene Informationen repräsentieren können, beispielsweise eine Audioinformation oder eine Videoinformation oder eine Kombination aus beiden oder eine Textinformation, wie beispielsweise Bücher oder Dokumente, und auch Kombinationen aus den zuvor erwähnten Informationen. Weiters sei erwähnt, dass selbstverständlich auch mehr als zwei digitale Daten D1 bzw. D2 vorliegen können.

Es sei weiters erwähnt, dass bei dem Kommunikationssystem 1 gemäß der Figur 1 die Kommunikation zwischen der Einrichtung 2 und der Datenquelle-Einrichtung 4 oder der Datensenke-Einrichtung 3 und bei dem System gemäß der Figur 2 die Kommunikation zwischen den beiden Kombinationseinrichtungen 24 und 25 auch auf kontaktlose Weise, wie beispielsweise über eine Funkverbindung, erfolgen kann.

Es sei erwähnt, dass die Einrichtung 2 und/oder die Datensenke-Einrichtung 3 und/oder die Datenquelle-Einrichtung 4 auch mit Hilfe von Personalcomputern realisiert sein können. Weiters sei erwähnt, dass auch die Einrichtung 2 als ein netzwerkfähiges Audio-Aufzeichnungs- und/oder Wiedergabegerät, wie beispielsweise einen MP3-Player/Rekorder, oder ein netzwerkfähiges Video-Aufzeichnung- und/oder Wiedergabegerät, wie beispielsweise einen Videorekorder, gebildet sein kann.

Patentansprüche:

1. Verfahren zum Verhindern einer unerwünschten Benutzung von digitalen Daten (D1, D2; D1', D2'), welche digitalen Daten (D1, D2; D1', D2') in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten (D1, D2; D1', D2') von einer Datenquelle-Einrichtung (4) für eine Datensenke-Einrichtung (3) zugänglich gemacht werden und welchen digitalen Daten (D1, D2; D1', D2') eine Blockierinformation (BL1, BL2; BL1', BL2') zugeordnet wird, mit deren Hilfe ein Verfügbarmachen der digitalen Daten (D1, D2; D1', D2') von der Datensenke-Einrichtung (3) für eine weitere Datensenke-Einrichtung blockierbar ist, welches Verfahren die nachfolgend angeführten Verfahrensschritte umfasst, nämlich

Verfügbarmachen einer Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für eine Datensenke-Einrichtung (3), welche Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') getrennt von den digitalen Daten (D1, D2; D1', D2') verfügbar gemacht wird und für ein Berechtigen des Benutzens der digitalen Daten (D1, D2; D1', D2') durch die Datensenke-Einrichtung (3) vorgesehenen ist und zumindest aus der Blockierinformation (BL1, BL2; BL1', BL2') und einer Entschlüsselungsinformation (DC1, DC2; DC1', DC2') besteht, welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2') den digitalen Daten (D1, D2; D1', D2') zugeordnet ist und mit welcher Entschlüsselungsinformation (DC1, DC2; DC1', DC2') die digitalen Daten (D1, D2; D1', D2') entschlüsselbar sind und welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2'), bevor die Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) verfügbar gemacht wird, für die Datenquelle-Einrichtung (4) verfügbar ist, und

Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4).

2. Verfahren nach Anspruch 1,

wobei das Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) durch ein Löschen der für die Datenquelle-Einrichtung (3) verfügbaren Entschlüsselungsinformation (DC1, DC2; DC1', DC2') erfolgt.

3. Verfahren nach Anspruch 1,

wobei zusätzlich eine Datensenkeinformation (SO) gemerkt wird, mit deren Hilfe die

Datensenke-Einrichtung (3) identifizierbar ist.

4. Verfahren nach Anspruch 1

wobei das Verfügbarmachen der Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) und das Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) in Abhängigkeit von einer ersten Beziehungsinformation (RI1), mit deren Hilfe eine Beziehung zwischen einem Benutzer (7) der Datenquelle-Einrichtung (4) und einem Benutzer (6) der Datensenke-Einrichtung (3) definierbar ist, entweder nur durch den Benutzer (7) der Datenquelle-Einrichtung (4) oder auch durch den Benutzer (6) der Datensenke-Einrichtung (3) veranlassbar ist.

5. Verfahren nach Anspruch 1,

wobei ein Beenden des Zugänglichmachens der digitalen Daten (D1, D2; D1', D2') für eine Datensenke-Einrichtung (3)
erstens das Verfügbarmachen der zuvor für die Datensenke-Einrichtung (3) verfügbar gemachten Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) und
zweitens das Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datensenke-Einrichtung (3) umfasst.

6. Verfahren nach Anspruch 5,

wobei das Beenden der Verfügbarkeit der digitalen Daten (D1, D2; D1', D2') für eine Datensenke-Einrichtung (3) in Abhängigkeit von einer zweiten Beziehungsinformation (RI2), mit deren Hilfe eine Beziehung zwischen einem Benutzer (7) der Datenquelle-Einrichtung (4) und einem Benutzer (6) der Datensenke-Einrichtung (3) definierbar ist, entweder nur durch den Benutzer (6) der Datensenke-Einrichtung (3) oder auch durch den Benutzer (7) der Datenquelle-Einrichtung (4) erfolgt.

7. Einrichtung (2) zum Verhindern einer unerwünschten Benutzung von digitalen Daten (D1, D2; D1', D2'), welche digitalen Daten (D1, D2; D1', D2') in verschlüsselter Form zur Verfügung stehen und welche digitalen Daten (D1, D2; D1', D2') von einer Datenquelle-Einrichtung (4) für eine Datensenke-Einrichtung (3) zugänglich machbar sind und welchen digitalen Daten (D1, D2; D1', D2') eine Blockierinformation (BL1, BL2; BL1', BL2') zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten (D1, D2; D1', D2') von der Datensenke-Einrichtung (3) für eine weitere

Datensenke-Einrichtung blockierbar ist,

wobei Verwaltungsmittel (9) vorgesehen sind, welche Verwaltungsmittel (9) zum Verfügbarmachen einer getrennt von den digitalen Daten (D1, D2; D1', D2') vorliegenden Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für eine Datensenke-Einrichtung (3) ausgebildet sind, welche Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für ein Berechtigen des Benutzens der digitalen Daten (D1, D2; D1', D2') durch die Datensenke-Einrichtung (3) vorgesehen ist und zumindest aus der Blockierinformation (BL1, BL2; BL1', BL2') und einer Entschlüsselungsinformation (DC1, DC2; DC1', DC2') besteht, welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2') den digitalen Daten (D1, D2; D1', D2') zugeordnet ist und mit welcher Entschlüsselungsinformation (DC1, DC2; DC1', DC2') die digitalen Daten (D1, D2; D1', D2') entschlüsselbar sind und welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2'), bevor die Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) verfügbar ist, für die Datenquelle-Einrichtung (4) verfügbar ist, und

wobei die Verwaltungsmittel (9) zum Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) ausgebildet sind.

8. Einrichtung (2) nach Anspruch 7,

wobei die Verwaltungsmittel (9) für das Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) zum Löschen der für die Datenquelle-Einrichtung (4) verfügbaren Entschlüsselungsinformation (DC1, DC2; DC1', DC2') ausgebildet sind.

9. Einrichtung (2) nach Anspruch 7,

wobei die Verwaltungsmittel (9) zusätzlich zum Merken einer Datensenkeinformation (SO) für die Datenquelle-Einrichtung (4) ausgebildet sind, mit deren Hilfe die Datensenke-Einrichtung (3) identifizierbar ist.

10. Einrichtung (2) nach Anspruch 7,

wobei die Verwaltungsmittel (9) zusätzlich zum Berücksichtigen einer ersten Beziehungsinformation (RI1) ausgebildet sind, mit deren Hilfe eine Beziehung zwischen einem Benutzer (7) der Datenquelle-Einrichtung (4) und einem Benutzer (3) der Datensenke-Einrichtung (3) definierbar ist, und

wobei die Verwaltungsmittel (9) ausgebildet sind, in Abhängigkeit von der durch die erste Beziehungsinformation (RI1) definierten Beziehung das Verfügbarmachen der Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) und das Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) entweder nur auf Veranlassung durch den Benutzer (7) der Datenquelle-Einrichtung (4) oder auch auf Veranlassung durch den Benutzer (6) der Datensenke-Einrichtung (3) zu ermöglichen.

11. Einrichtung (2) nach Anspruch 7,

wobei für ein Beenden der Verfügbarkeit der digitalen Daten (D1, D2; D1', D2') für die Datensenke-Einrichtung (3) die Verwaltungsmittel (9) zum Verfügbarmachen der zuvor für die Datensenke-Einrichtung (3) verfügbar gemachten Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) und zum Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datensenke-Einrichtung (3) ausgebildet sind.

12. Einrichtung (2) nach Anspruch 11

wobei die Verwaltungsmittel (9) zusätzlich zum Berücksichtigen einer zweiten Beziehungsinformation (RI2) ausgebildet sind, mit deren Hilfe eine Beziehung zwischen einem Benutzer (7) der Datenquelle-Einrichtung (4) und einem Benutzer (6) der Datensenke-Einrichtung (3) definierbar ist, und

wobei die Verwaltungsmittel (9) ausgebildet sind, in Abhängigkeit von der durch die zweite Beziehungsinformation (RI2) definierten Beziehung das Beenden der Verfügbarkeit der digitalen Daten (D1, D2; D1', D2') für die Datensenke-Einrichtung (3) entweder nur auf Veranlassung des Benutzers (6) der Datensenke-Einrichtung (3) oder auch auf Veranlassung durch den Benutzer (7) der Datenquelle-Einrichtung (4) zu ermöglichen.

13. Datensenke-Einrichtung (3) zum Benutzen digitaler Daten(D1, D2; D1', D2'), welche digitalen Daten (D1, D2; D1', D2') in verschlüsselter Form verfügbar sind und welche digitalen Daten (D1, D2; D1', D2') von einer Datenquelle-Einrichtung (4) für die Datensenke-Einrichtung (3) zugänglich machbar sind und welchen digitalen Daten (D1, D2; D1', D2') eine Blockierinformation (BL1, BL2; BL1', BL2') zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten (D1, D2; D1', D2') von der Datensenke-Einrichtung (3) für eine weitere Datensenke-Einrichtung blockierbar ist,

wobei erste Verarbeitungsmittel (16) vorgesehen sind, die unter Berücksichtigung eines

ihnen zuführbaren ersten Ermöglichungssignals (ES1), welches erste Ermöglichungssignal (ES1) ein Verarbeiten der digitalen Daten (D1, D2; D1', D2') durch die ersten Verarbeitungsmittel (16) ermöglicht, und unter Ausnutzung einer Entschlüsselungsinformation (DC1, DC2; DC1', DC2'), welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2') den digitalen Daten (D1, D2; D1', D2') zugeordnet ist und mit deren Hilfe die digitalen Daten (D1, D2; D1', D2') entschlüsselbar sind, für das Verarbeiten der digitalen Daten (D1, D2; D1', D2') ausgebildet sind, und

wobei erste Prüfmittel (15) vorgesehen sind, die erstens zum Zusammenwirken mit einer Einrichtung (2) nach einem der Ansprüche 7 bis 12 ausgebildet sind und die zweitens zum Prüfen ausgebildet sind, ob eine Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) verfügbar ist, welche Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') getrennt von den digitalen Daten (D1, D2; D1', D2') existiert und für das Berechtigen des Benutzens der digitalen Daten (D1, D2; D1', D2') durch die Datensenke-Einrichtung (3) vorgesehen ist und zumindest aus der Blockierinformation (BL1, BL2; BL1', BL2') und der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') besteht und vor dem Verfügbarmachen der Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) der Datenquelle-Einrichtung (4) verfügbar ist, und die drittens bei einem Vorliegen eines positiven Prüfergebnisses zum Erzeugen des ersten Ermöglichungssignals (ES1) und zum Abgeben des ersten Ermöglichungssignals (ES1) an die Verarbeitungsmittel (16) ausgebildet sind, und

wobei erste Blockiermittel (18) vorgesehen sind, die unter Berücksichtigung der Blockierinformation (BL1, BL2; BL1', BL2') zum Blockieren eines Verfügbarmachens der digitalen Daten (D1, D2; D1', D2') für eine weitere Datensenke-Einrichtung ausgebildet sind.

14. Datensenke-Einrichtung (3) nach Anspruch 13,

welche Datensenke-Einrichtung (3) eine Einrichtung (2) nach einem der Ansprüche 7 bis 12 enthält.

15. Datenquelle-Einrichtung (4)

zum Verfügbarmachen von digitalen Daten (D1, D2; D1', D2') für eine Datensenke-Einrichtung (3), welche digitalen Daten (D1, D2; D1', D2') in verschlüsselter Form

verfügbar sind und welchen digitalen Daten (D1, D2; D1', D2') eine Blockierinformation (BL1, BL2; BL1', BL2') zugeordnet ist, mit deren Hilfe ein Verfügbarmachen der digitalen Daten (D1, D2; D1', D2') von der Datensenke-Einrichtung (3) für eine weitere Datensenke-Einrichtung blockierbar ist,

wobei zweite Verarbeitungsmittel (22) vorgesehen sind, die unter Berücksichtigung eines ihnen zuführbaren zweite Ermöglichungssignals (ES2), welches zweite Ermöglichungssignal (ES2) ein Verarbeiten der digitalen Daten (D1, D2; D1', D2') durch die zweiten Verarbeitungsmittel (22) ermöglicht, und unter Ausnutzung einer Entschlüsselungsinformation (DC1, DC2; DC1', DC2'), welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2') den digitalen Daten (D1, D2; D1', D2') zugeordnet ist und mit deren Hilfe die digitalen Daten (D1, D2; D1', D2') entschlüsselbar sind, für das Verarbeiten der digitalen Daten (D1, D2; D1', D2') ausgebildet sind, und

wobei zweite Prüfmittel (21) vorgesehen sind, die erstens zum Zusammenwirken mit einer Einrichtung (2) nach einem der Ansprüche 7 bis 12 ausgebildet sind und die zweitens zum Prüfen ausgebildet sind, ob eine Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) verfügbar ist, und die drittens bei einem Vorliegen eines positiven Prüfungsergebnisses zum Erzeugen des zweiten Ermöglichungssignals (ES2) und zum Abgeben des zweiten Ermöglichungssignals (ES2) an die zweiten Verarbeitungsmittel (22) ausgebildet sind.

16. Datenquelle-Einrichtung (4) nach Anspruch 15,

welche Datenquelle-Einrichtung (4) eine Einrichtung (2) nach einem der Ansprüche 7 bis 12 enthält.

17. Kombinationseinrichtung (24, 25) mit einer Datenquelle-Einrichtung und einer Datensenke-Einrichtung,

welche Kombinationseinrichtung (24, 25) eine Datenquelle-Einrichtung (4) nach einem der Ansprüche 13 bis 14 und

eine Datensenke-Einrichtung (3) nach einem der Ansprüche 15 bis 16 enthält.

Zusammenfassung

Verfahren und Einrichtung zum Verfügbarmachen von verschlüsselten digitalen Daten

Bei einem Verfahren zum Verhindern einer unerwünschten Benutzung von verschlüsselten digitalen Daten (D1, D2; D1', D2') ist vorgesehen, dass eine Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für eine Datensenke-Einrichtung (3) verfügbar gemacht wird, welche Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') getrennt von den digitalen Daten (D1, D2; D1', D2') verfügbar gemacht wird und für ein berechtigtes Benutzen der digitalen Daten (D1, D2; D1', D2') durch die Datensenke-Einrichtung (3) vorgesehen ist und zumindest aus der Blockierinformation (BL1, BL2; BL1', BL2') zum Blockieren eines weiteren Verfügbarmachens der digitalen Daten (D1, D2; D1', D2') und einer Entschlüsselungsinformation (DC1, DC2; DC1', DC2') besteht, welche Entschlüsselungsinformation (DC1, DC2; DC1', DC2') den digitalen Daten (D1, D2; D1', D2') zugeordnet ist und zum Entschlüsseln der digitalen Daten (D1, D2; D1', D2') vorgesehen ist und, bevor die Benutzungsberechtigungsinformation (BBI1, BBI2; BBI1', BBI2') für die Datensenke-Einrichtung (3) verfügbar gemacht wird, für die Datenquelle-Einrichtung (4) verfügbar ist, und bei welchem Verfahren weiters ein Entziehen der Verfügbarkeit der Entschlüsselungsinformation (DC1, DC2; DC1', DC2') für die Datenquelle-Einrichtung (4) erfolgt.

(Figur 1)

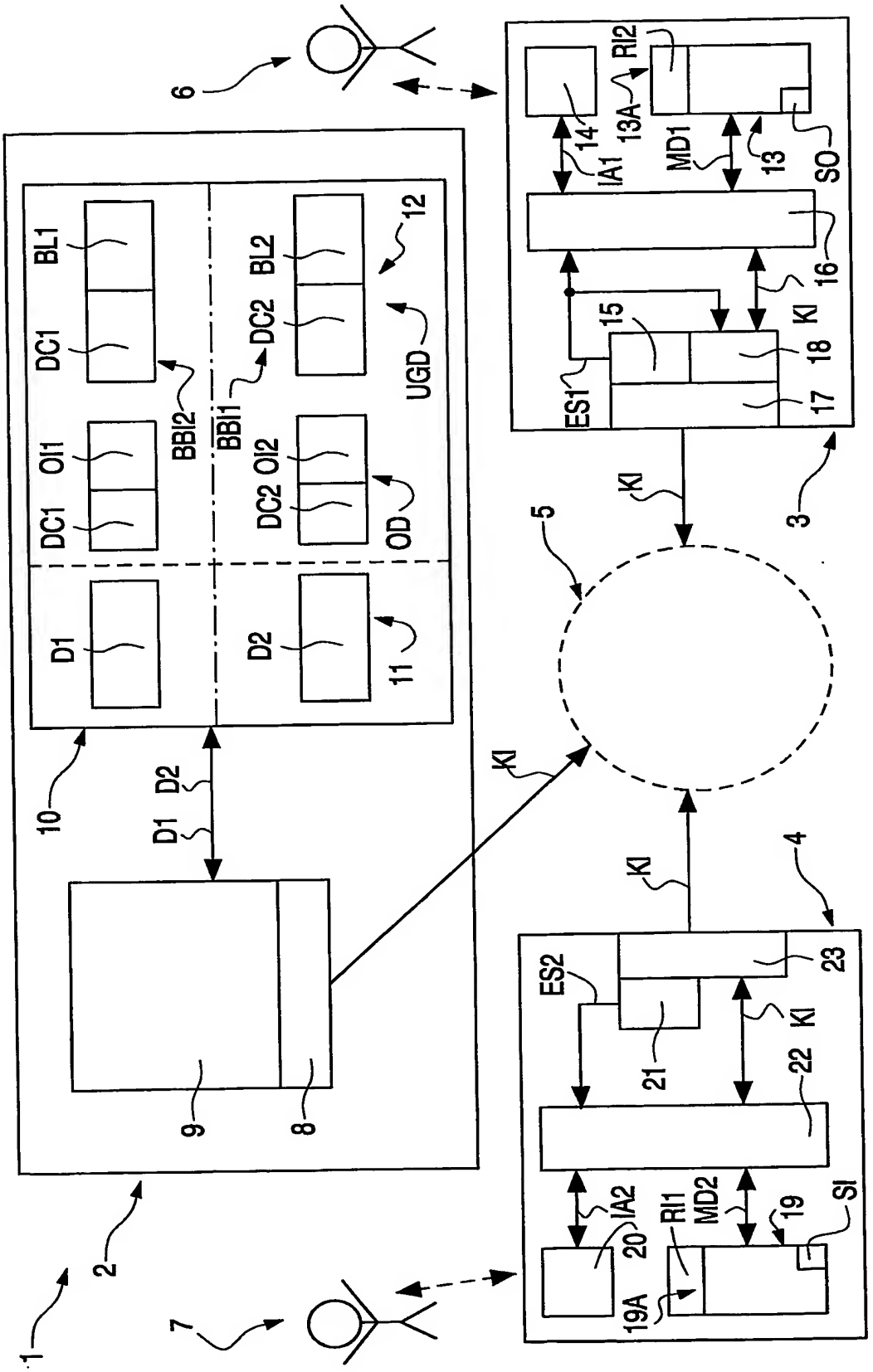
1
2
3
4
5
6
7
8
9
10
11
12
13
13A
14
15
16
17
18
19
19A
20
21
22
23
BL1
DC1
OI1
DC1
D1
BBI2
BBI1
BL2
DC2
DC2 OI2
D2
UGD
OD
D2
D1
KI
KI
KI
KI
RI2
IA1
MD1
SO
ES1
KI
ES2
KI
IA2
RI1
MD2
SI

Fig.1

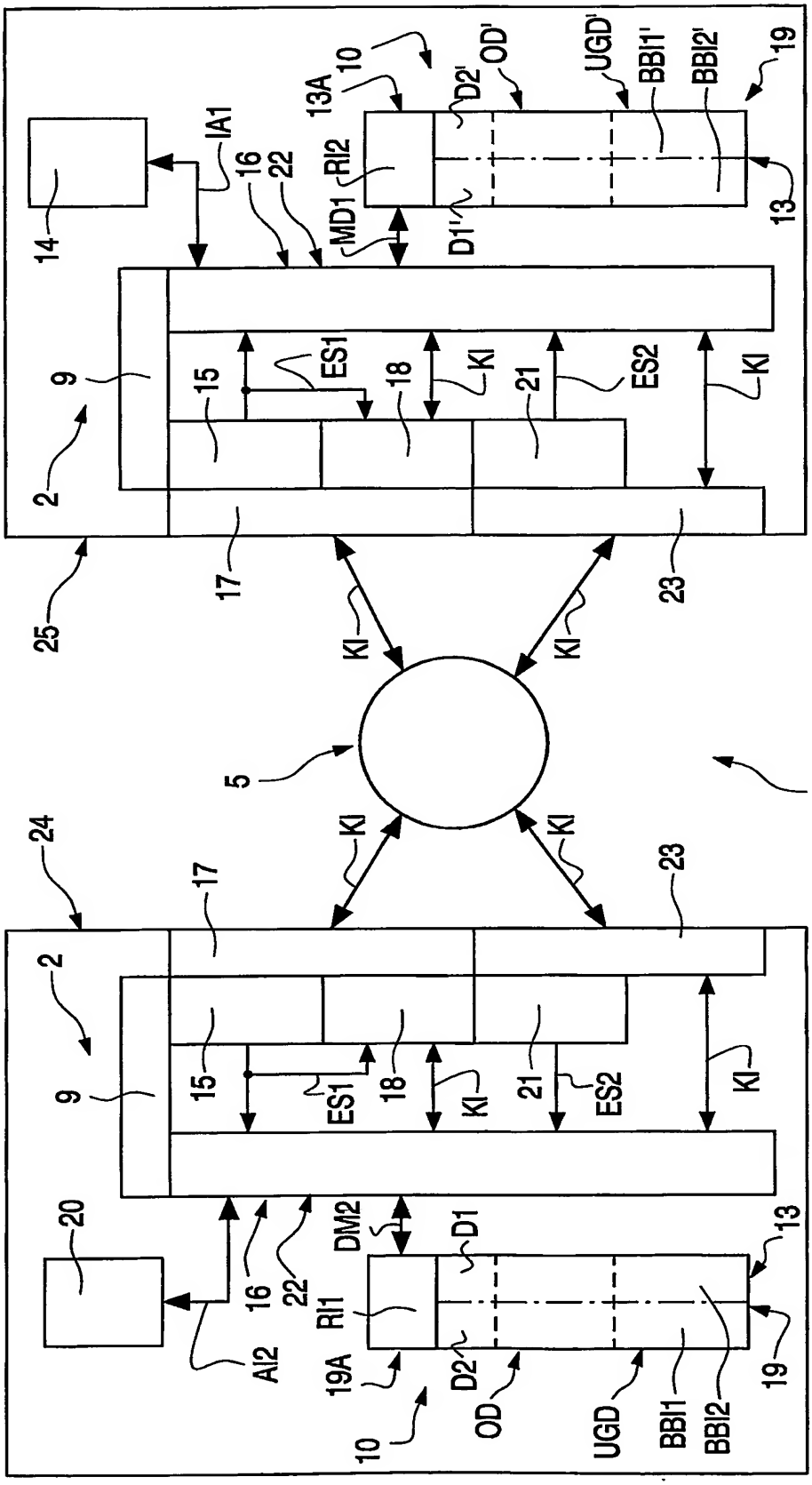
1
2
5
9
10
13
13A
14
15
16
17
18
19
19A
20
21
22
23
24
25
ES1
ES2
KI
IA1
RI2
MD1
D1'
D2'
OD'
UGD'
BBI1'
BBI2'
DM2
D1
RI1
AI2
D2
OD
UGD
BBI1
BBI2

Fig.2

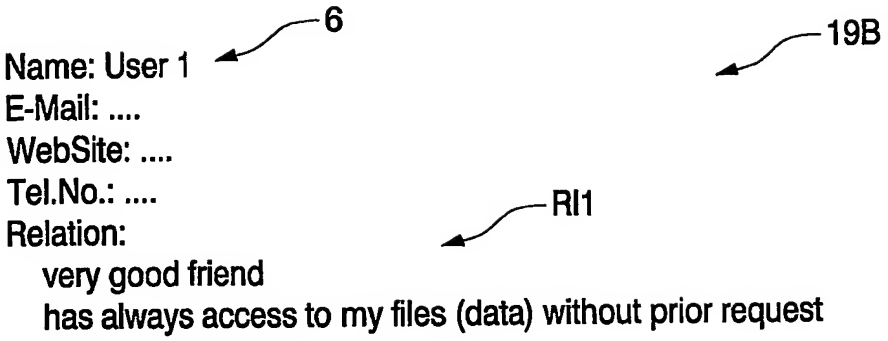
6
19B
Name: User 1
E-Mail: ....
WebSite: ....
Tel.No.: ....
Relation:
RI1
very good friend
has always access to my files (data) without prior request

Fig.3

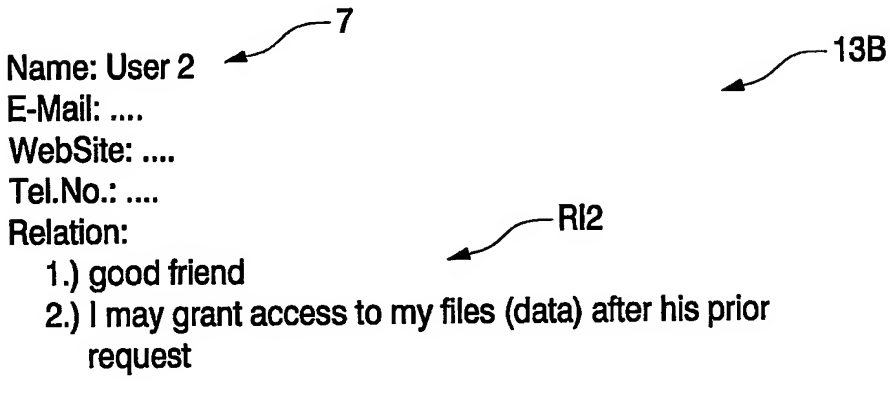
7
13B
Name: User 2
E-Mail: ....
WebSite: ....
Tel.No.: ....
Relation:
RI2
1.) good friend
2.) I may grant access to my files (data) after his prior request

Fig.4